Chapter 6

Configuring Notification Objects

Overview

Introduction

Use the Notification Objects Configuration page to create groups that you want Proventia Network ADS to notify when it generates alerts. You can group similar members (for example, all of your network security engineers) together so they all receive the same types of event notifications.

User access on the Notification page

Users with administrative privileges can perform all the actions described in this chapter. Analysts can create and edit notification objects. Regular users can view the notification object configuration, but cannot change it.

In this chapter

This chapter contains the following topics:

About the Notification Objects Configuration Page

Introduction

The Notification Objects Configuration page shows all of the configured notification objects and their settings. After you create a notification object, the system displays it as a selection choice when you define alerting for behaviors and rules.

Navigating and searching on the Notification page

You can search for an object name, the creator of an object, or any object destination or see examples of search entries. Standard navigation and searching applies on the Notification Configuration page.

Reference: See "Navigating the Proventia Network ADS Web User Interface" on page 12.

Notification object table

The table shows the following information for each notification object:

Column	Description
Name	The object name, as a link to the Edit page.
Email	The list of To email addresses for the users who receive email alerts and the From email address from which the email notifications appear to be sent.
SNMP	The configured SNMP destination, community, and version.
Syslog	The configured destination, facility, and severity uses to send syslog alerts.
Comments	Any comments entered when the object was created.
Log Message	The most recent logged message for this object.
Creator	The user who created the notification object.
Last Modified	The last time any changes were made to this object.
Policy Referrers	The names of the rules that reference this object as links to the corresponding Rule Editor page.
Alerting Referrers	The names of alert behaviors that reference this object, as links to the corresponding Alert Configuration page.
Selection check box	Use to delete objects.

Table 16: *Notification objects table*

About MIBs

You can download and view the Proventia Network ADS and SMI Managed Information Base files (MIBs) for SNMP versions 1 and 2. The MIB files define the format of ISS SNMP traps and is used by your management application to provide translations of the numeric Object Identifiers (OIDs) contained in the trap messages.

Viewing MIBs

To see the MIB:

- Click the corresponding link for the MIB you want to download.

  Depending upon your browser, the system either displays the MIB in a new window, or the Save As window for you to choose where to save the MIB file.

Saving MIBs

To save the MIB:

1. Specify the file location.
2. Click **SAVE.**
3. If you view the MIB file in a new window, click your browser's **Back** button to return to the prior page.

Adding change messages on the Notification Object Configuration page

You should enter a change message when you make changes to a notification object. The system displays these messages as part of the log pages and the recent changes for reference.

Viewing recent changes

The Notification Objects Configuration page displays a list of the most recent notification changes for you to reference.

To see a complete list of all notification object changes:

- Click the Full change log for Notification Object link to navigate to the Log Detail page.

Notification Types

Introduction

This topic describes the different types of notifications you can set for notification objects, and how Proventia Network ADS uses the objects to send the event notifications.

About notification types

For each notification object you create, you specify a notification type which tells the system how to send event notifications when it detects unapproved behavior. You can create notification objects that include email notifications, SNMP traps, syslog messages, or a combination of the three, and then specify the recipients for each notification type.

How Proventia Network ADS uses notification objects

Proventia Network ADS does not come with default notification objects. You must create them on the Edit Notification Object page. After you have created notification objects, the system displays them as a selection choice in the alert configuration for the built-in and user-defined rules. This allows you to selectively apply notification objects to different behaviors and to customize alerting.

SiteProtector notifications

If you configure your ADS to integrate with SiteProtector, it sends SiteProtector event notifications automatically. Any notification objects you apply to rules are additional.

About email notifications

Proventia Network ADS sends email notifications to the destination address you specify, and the notifications appear to come from the sender address. The system queues email messages for one minute, and then sends them in a batch. When an email notification contains multiple alerts, the system sends one summary notification that contains the individual email messages. The messages include the behavior it references, the severity, expected rates, and a URL you can copy and paste into your browser to navigate directly to the event.

The system sends email notifications through the SMTP server you configure on the General Settings page in the Settings menu.

For an example of all types of email notifications Proventia Network ADS sends, see "Appendix A: Notification Formats" in the *Proventia Network Advanced Configuration Guide.*

About SNMP notifications

Proventia Network ADS supports SNMP versions 1 and 2. Proventia Network ADS uses both the ISS and Proventia Network ADS MIBs to send traps.

Reference: See "Viewing MIBs" on page 38.

About syslog notifications

When the system sends syslog alerts, it displays the alert type at the beginning of the message, followed by the alert details. The sylog messages include the behavior it references, the severity, expected rates, and a URL you can copy and paste into your browser to navigate directly to the event.

Adding and Editing Notification Objects

Introduction

This topic provides instructions for adding and editing notification objects. Because the pages for adding and editing group objects are similar, they are addressed here together.

Naming notification objects

ISS recommends that you choose a unique name for each notification object so that you can easily identify it when you are defining event rules. You can use any number/letter combination, and valid names must include at least one character.

Configuring notification objects

To configure a notification object:

1. Do one of the following to navigate to the edit page:
   - Click **NEW NOTIFICATION OBJECT** to add a new object.
   - Click the notification object name link to change the settings for an existing notification object.

   Note: You can also navigate to the Edit Notification Objects page from the Edit Alert Configuration page.
2. Type a name for the object in the **Name** box.

   Reference: See "Naming notification objects" above.
3. Type any text that describes the group in the **Comment** box.

   The system includes these comments in the table on the Notification Object Configuration page.
4. Choose the types of notifications you want to include in this object.
5. Follow the on-screen instructions for adding email, SNMP, and syslog notifications.
6. Type a message that describes your changes in the **Change Message** box.
7. Click **SAVE**.

Adding email notifications

For email notifications, all email addresses you enter must be valid RFC822 addresses.

To enter an email address:

1. Type the recipient's email address in the **To** box.

   Note: Enter multiple recipients as a comma-separated list of email addresses.
2. Type the sender's email address in the **From** box.

   Tip: You might want to use the Proventia Network ADS Analyzer name to easily identify any messages sent.

Adding SNMP notifications

To add SNMP notifications:

1. Type the IP address for each SNMP TRAP receiver in the **Destination IP** box.

   Note: Enter multiple trap receivers as a comma-separated list of IP addresses.
2. Type the IP address for the SMNP agent in the **Agent IP** box.
3. Type a community string if your organization's SNMP configuration requires one. Otherwise, the system defaults to the standard public setting.
4. Select the SNMP version you use from the **Version** list.

Adding syslog notifications

To add syslog notifications

1. Enter each syslog host IP address in the **Destination IP** box.

   Note: Enter multiple syslog destinations as a comma-separated list of IP addresses.

2. Select a facility value from the list.

   Note: Daemon is the default facility.

3. Select a severity value from the list.

   Note: Emergency is the default severity.

Deleting Notification Objects

Introduction

You can only delete a notification object from the Notification Objects Configuration page.

Deleting objects with rule referrers

If a notification object that you are deleting is part of any policy rule, the system displays a message showing you the number of rules that reference this object. This allows you to cancel the action if necessary.

Procedure

To delete a notification object:

1. Select the check box on the notification row in the table.
2. Type a description that explains why you are deleting an object in the **Change Message** box.
3. Click **DELETE**.

   If the system displays the rule referrer message, click **OK** to continue, and then delete the object.

Chapter 7

Configuring Time Objects

Overview

Introduction

The Time Objects page shows all of the time specifications that you can use in alert configuration. Proventia Network ADS creates events for violations when they occur during configured time objects.

Example: If you want to be notified if the system detects new service alerts on work days, create a time object for Monday through Friday during work hours and select it in the alert configuration for new services.

User access on the Time Objects page

Administrators can perform all actions described in this chapter. Analysts can create and edit time objects. Users can view the time objects but cannot change them.

In this chapter

This chapter contains the following topics:

About the Time Objects Page

Introduction

The Time Objects page shows all configured time objects and their configured settings. Once you create a time object, the system displays it as a selection choice when you define alerting for behaviors and rules.

Navigating and searching on the Time Objects page

You can search for an object name, the creator of the object, or see examples of search entries. Standard navigation and searching applies on the Time Object page.

Reference: See "Navigating the Proventia Network ADS Web User Interface" on page 12.

Time objects table

The table shows the following information for each time object:

Column	Description
Name	The name of the object, as a link to its Edit page, where you can make changes.
Specification	The days and hours that define the object.
Comment	Any comments that you entered when you created the object.
Log Message	The most recent logged message for this object.
Creator	The user who created the object
Last Modified	The last time changes were made to the object.
Rule Referrers	The number of rules that reference this time object, as links. If this time object references multiple rules, the system displays an ellipsis point link (...) that navigates to the Edit page, where each individual rule is listed as a link to its corresponding Rule Editor page.
Selection check box	Use to select specific time objects to delete or include in export files.

Table 17: *Time object table*

Adding change messages on the Time Objects page

You should enter a change message when you make changes to a time object. The system displays these messages as part of the log pages and the recent changes for reference.

Viewing recent changes

The Time Objects page displays a list of the most recent time object changes for you to reference. To see a complete list of all time object changes:

- Click the Full change log for Time Object link to navigate to the Log Detail.

Adding and Editing Time Objects

Introduction

This topic provides the instructions for adding and editing time objects. Because the pages for adding and editing time objects are similar, they are addressed here together.

About the Time Objects page

The Edit Time Objects page allows you to create and edit time objects, or blocks of time, that you then use for alert configuration. Proventia Network ADS creates events for rule violations when they occur during your set time objects.

Naming time objects

ISS recommends that you choose a unique name for each time object so that you can easily identify when defining event rules. You can use any number/letter combination and valid names must include at least one character.

Configuring time objects

To configure a time object:

1. Do one of the following to navigate to the Edit page:
   - Click **NEW TIME OBJECT** to add a new object.
   - Click the name link to change the settings for an existing time object.

   Note: You can also navigate to the Edit Time Object page from the Edit Alert Configuration page.
2. Type a name for the object in the **Name** box.

   Reference: See "Naming time objects" above.
3. Type any text that describes the object in the **Comment** box.

   The system includes these comments in the table on the Time Object page.
4. Select the check boxes for the days of the week you want this time period to apply to.
5. Enter the start and end time for the object.

   Tip: You can specify multiple objects for a single time block by adding multiple rows.
6. Select the appropriate time zone from the list.
7. Type a message that describes your changes in the **Change Message** box.
8. Click **SAVE**.

About start and end times

If you enter an end time that is earlier than the start time, the system assumes the time object runs overnight and into the next day.

Example: If you enter 22:00 to 02:00, the system assumes that this time object runs from 10:00 p.m. through 2:00 a.m. the next day, and accepts this as a valid entry.

Deleting Time Objects

Deleting objects with rule referrers

If a time object that you are deleting is part of any policy rule, the system displays a message showing you the number of rules that reference this object. This allows you to cancel the action if necessary.

Procedure

To delete a time object:

1. Select the check box on the times row in the table.
2. Type a description that explains why you are deleting an object in the **Change Message** box.
3. Click **DELETE**.

   If the system displays the rule referrer message, click **OK** to continue, and then delete the object.

Chapter 8

Configuring Group Objects

Overview

Introduction

You can specify groups of network addresses you want Proventia Network ADS to monitor together on the Group Configuration page.

Navigating on the Group page

Standard navigation and searching apply on the Group Configuration page.

Reference: See "Navigating the Proventia Network ADS Web User Interface" on page 12.

User access for group configuration

Administrators can perform all actions described in this chapter. Analysts can create and edit groups. Regular users can view the group configuration, but they cannot edit it or add change messages.

In this chapter

This chapter contains the following topics:

About the Group Objects Configuration Page

Introduction

The Configure Group Object page displays all of the configured groups in your network. Each group object represents a user-defined block of address space.

Groups table

The Groups table shows the following information for each group listed on this page:

Column	Description
Group	The name of the group object, as a link to the edit page.
Members	The names or addresses of the group members. If the number of members exceeds five lines, this column shows an ellipsis point link (...) that you can click to navigate to the Edit page to see the complete list of members.
Severity	The user-assigned severity level Proventia ADS uses when creating alerts that involve this group.
Comment	Any comments entered when the group object was created.
Log Message	The most recent logged message for this group object.
Creator	The name of the user who created the group object.
Last Modified	The last time the group was changed (this includes system-generated changes).
Report Aggregate	Displays Yes or No to indicate if the group is set as an aggregate for searching traffic. **Reference:** See "Searching over aggregated group objects" on page 102.
Rule Referrers	The names of all rules that reference this group object, as links to the Edit page.
Group Referrers	The names of all other group objects that reference this group, as links to the edit page.
Selection check box	Use to delete group objects.

Table 18: *Group objects table*

About change messages

You should enter a change message when you make changes to a group object. The system displays these messages as part of the log pages and the recent changes for reference.

Viewing recent changes

The Group Objects Configuration page displays a list of the most recent notification changes for you to reference. To see a complete list of all notification object changes:

- Click the Full change log for Group link to navigate to the Log Detail.

Adding and Editing Group Objects

Introduction

This topic provides the instructions for adding and editing group objects. Because the pages for adding and editing group objects are similar, they are addressed here together.

About group contents

Use the Edit Group Objects pages to update any existing groups or add new groups to define a block of address space. When defining a group, you can enter overlapping group contents. This means you can make one group that belongs to one or more other groups by specifying the group name instead of the IP address or CIDR. When group members are other groups, the system displays their assigned group names in the table instead of their addresses.

Naming group objects

When you add a group, you assign it a name. ISS recommends assigning each group a unique name that allows you to easily identify its members. Valid names must include at least one character. The following list shows all of the characters you can use in a group name:

- any letters (capital or lowercase)
- any whole numbers (0-9)
- spaces
- colon (:)
- period (.)
- hyphen (-)
- question mark (?)
- pipe (|)
- parentheses ( )
- number/pound sign (#)
- asterisk (*)
- plus sign (+)
- equal to sign (=)

Using the report aggregate option

The Report Aggregate group option provides you with another way to filter the results that the system displays. This option allows you to narrow your search by choosing a group for Proventia Network ADS to use when it aggregates traffic. When you aggregate traffic by a specific group, the system only looks at the traffic over that group space instead of over the whole network (Auto).

Example

The Mariner network has a group, named "Nautical," that contains five CIDR blocks. The "Nautical" group is a group the system can aggregate by—the Report Aggregate check box is selected on the Edit Groups page, so the Nautical group name appears as a choice in the Aggregate by list on the Explore page.

If you select the Nautical group to aggregate by when you search, the system aggregates traffic up to only the members of the Nautical group, and only displays traffic results related to that group. It shows the five CIDR blocks in traffic tables that are part of the Nautical group, and each block's associated traffic. This does mean, however, that if you

search over a network that the Nautical group is not a part of, the system does not show any traffic in the search results.

Note: The system can only aggregate by a group if you select the Report Aggregate check box for the group on the Edit Groups page.

Procedure

To add or edit groups:

1. Do one of the following to navigate to the Edit Group Objects page:
   - Click **NEW GROUP OBJECT** to add a new object.
   - Click the name link for the group object to change settings for an existing group object.

   Note: You can also navigate to the Edit Group Objects page from the Time Objects page and from the Policy page.
2. Type a name for the group object in the **Name** box.

   Group names can contain spaces.

   Reference: See "Naming group objects" on page 51.
3. Type any comments that describe the group or that help you identify it in the **Comment** box.

   Proventia Network ADS displays the text you enter here in the Comment field on the pages that include groups in the data tables.
4. Type the group addresses as a CIDR block, a single range, names of existing group objects, or a comma-separated list for the addresses you want Proventia Network ADS to monitor in the **Members** box.

   Tip: For multiple ranges, you can either add a new line for each range or enter a comma-separated list.

   Note: You can also specify members you want to exclude by negating a member.

   Example: `! 10.0.1.5` means not IP address 10.0.1.5.
5. Select the **Report Aggregate** check box if you want this group to be used for aggregating traffic on the Explore and Policy pages.
6. Select the severity you want to associate with this group.

   Any time this group is involved in alert traffic, the system uses this setting to flag the alert, unless there is a higher setting associated with the alert. The system always uses the highest setting when sending alerts.
7. Type any messages that describe the changes in the **Change Message** box.

   These messages appear in the log pages that include this group object.
8. Click **SAVE**.

Importing and Exporting Group Object Files

Introduction

When you add or edit a group object, you can import existing comma-separated value (CSV) files that you can use to create new groups or to merge into existing groups. Exporting a group object file allows you to see an example of the file format or to back up your network configuration within the system. You can also import and export a group file to use when you set up a new Proventia Network ADS system or for archival purposes.

Note: Proventia Network ADS accepts any CSV file that includes group names.

How Proventia Network ADS merges imported groups

This table shows how Proventia Network ADS merges imported groups:

If the group...	Then ADS...
exists, but is different	updates (overwrites) the old information.
exists, but is the same	ignores it.
does not exist	adds it.

Table 19: *Merge results for group objects*

Importing group files

To import a file:

1. Do one of the following:
   - Enter the file name in the box.
   - Click **Browse**, and then select the file to be included.
2. Type a description that explains why or what objects you are importing in the **Change Message** box.
3. Click **IMPORT**.

   The system displays a confirmation message when it finishes importing that shows how many groups it successfully added and how many it ignored, and then shows the new group information in the group data table.

Importing SiteProtector groups

When you import groups from SiteProtector, the Analyzer imports all groups; you can not selectively import them. If you have a group in ADS that is named the same as a SiteProtector group, when the groups are imported, the SiteProtector group overwrites the ADS group with the same name.

SiteProtector group object names

When group object names in SiteProtector do not match the allowed ADS group object name format, Proventia Network ADS changes the names as follows:

If the SiteProtector Group Object Name...	Then ADS...
starts with anything other than a letter (including IP addresses and IP ranges)	prepends the name with "SP." **Example:** 37North would become SP37North.
contains invalid characters	replaces the characters with a space.

Table 20: *SiteProtector group object names*

If the SiteProtector Group Object Name...	Then ADS...
includes duplicate names within different hierarchy levels	renames the group object by expanding the hierarchy name. **Example:** If there are two groups named "Admin," one in the Chicago group and one in the Atlanta group, because ADS doesn't allow two groups named Admin, it would rename them as follows: • Admin(of Chicago) • Admin(of Atlanta)
is called "any"	prepends the name with "SP."

Table 20: *SiteProtector group object names (Continued)*

Exporting group files

To export a file:

1. Type a description that explains why or what objects you are exporting in the **Change Message** box.
2. Click **EXPORT**, and then specify how you want to save or open the file, according to the choices your browser displays.

   Proventia Network ADS generates an XML report containing the group list to the location you specify.

Deleting Group Objects

Introduction

Delete groups on the Configure Group Objects page.

Deleting group objects with rule referrers

When you delete a group object, if that group is part of any policy rules, the system displays a message showing you the number of rules this group refers to. This allows you to cancel the action if necessary.

Procedure

To delete a group:

1. Select the check box on the group row in the table.
2. Type a description that explains why you are deleting an object in the **Change Message** box,
3. Click **DELETE**.

   If the system displays the rule referrer message, click **OK** to continue, and then delete the group.

Chapter 9

Configuring Policy Settings

Overview

Introduction

The Policy page shows all the alert categories that Proventia Network ADS detects. This includes built-in and ATF behaviors and any user-defined rules. This chapter contains information about the different behaviors, types of alerting, and the instructions for configuring policy alerting.

Navigating on the Policy pages

Standard navigation and searching apply on the Policy Settings page.

Reference: See "Navigating the Proventia Network ADS Web User Interface" on page 12.

User access on the Policy pages

Regular users and analysts can view the policy and ATF settings, but cannot edit them. For administrators, the Policy page shows rule names and associated event icons that link to additional pages of information. These are not available for users and analysts.

In this chapter

This chapter contains the following topics:

About the Policy Page

Introduction

The Policy page shows the different types of behaviors Proventia Network ADS tracks, and allows you to update alerting settings.

Viewing behavior tables

The Policy page shows tables with the current settings for the behaviors that the system applies to all new alerts. There is a table for built-in behaviors, ATF behaviors, System events, and for user-defined rules. The tables are similar and are described here together. Not all columns are shown for each table.

The tables show the following information:

Column	Description
Behavior	The name of the behavior category.
Severity	The severity level associated with the behavior.
Alerting	The types of alerting that the system is currently creating events for when it detects violations of this behavior.
Description	The behavior description, either system-generated or user-defined, depending upon the behavior.
Creator	The name of the user who created the rule or "system" or "ATF" for system-generated behavior rules.
Notification	The user-configured destinations where the system is sending event notifications.
Selection box	Use this check box to select and delete ATF and user-defined behavior rules.

Table 21: *Policy behavior table*

How ADS generates ATF behavior rules

The ISS security team updates the ATF when they discover new threats. You can enable automatic ATF updates, and then set how often your Proventia Network ADS Analyzer polls the threat feed for updates. When the system retrieves updates, it correlates the threat feed data with your network activity and creates appropriate policy.

Viewing Active Threat Feed behaviors

The Active Threat Feed Behaviors table shows all policies the system generates from the ATF data and allows you to enable automatic ATF updates. Use the scroll bar to the right of the ATF Behavior table to view all ATF policies listed in the table.

Reference: See "Configuring Active Threat Feed Settings" on page 71 for information about configuring, deleting, and recreating ATF behaviors.

Viewing user-defined rules

User-defined rules shows the settings for any rules users have created for your network. Use the scroll bar to the right of the user-defined rules table to view all rules listed in the table.

Viewing recent changes

The Recent Changes table displays a list of the most recent behavior changes for you to reference. The table provides the following information:

Column	Description
Time	The date and time the change was made.
User	The user who made the change.
Action	The type of change made: add, edit or delete.
Object	The affected object type: time object, notification object, rule, or group object.
Name	The name of the affected object.
Message	Any log messages the user entered when making the change, or the auto-generated system message for automatic changes.
Revision	The number of this revision to the object.

Table 22: *Recent changes table*

Viewing all rule changes

To see the complete list of all rule changes:

- Click the Full change log for Policies link to navigate to the Log Details page.

  Reference: See "Viewing Log Details" on page 132 for a description of the Log page.

Navigating to alert and notification configuration

The system displays each alert category in the Built-in Behaviors and the System Events tables as a link to its Edit Alerting and Notification page. From here, you can enable alerting and specify how you want the system to notify you of behavior violations. This allows you to customize alerting to make sure the system sends alerts for the types of events and categories of behavior you deem important.

Reference: See "Configuring Alerting Settings for Built-in Behaviors" on page 65.

Navigating to the Rule Editor

The system displays each rule name in the ATF and User-created rules tables, and in the Recent Changes table, as a link to the Rule Editor page for that specific rule. Use the Rule Editor page to update a rule, including the time and notification objects and the alert configuration.

Reference: See "Creating and Editing Rules" on page 117.

Navigating to the Event Details page

The system displays a View Event link in the ATF and User-created rules tables. Use the Event Details page to see the involved clients, servers, services, and a graph of the activity for a specific event.

Reference: See "Viewing Event Details" on page 114 for more information about viewing events.

How Proventia Network ADS Determines Severity

Introduction

This topic describes the severity levels and provides examples of severity levels associated with different types of alerts.

About severity settings

Use the severity settings to specify the severity level you want Proventia Network ADS to associate with each alert type (traffic violation, over, under, or rate alert). The system uses the severity setting to rank the alerts that appear on the Summary page and includes the severity setting in the notifications it generates. You can also use the Severity setting to sort or search for alerts. The severity settings range from 1-10, as follows:

- The system considers severity settings of 8-10 as high, and displays alerts of this severity level in tables with a red icon.
- The system considers severity settings of 5-7 as medium, and displays alerts of this severity in tables with a yellow icon.
- The system considers severity settings of 1-4 as low, and displays alerts of this severity in tables with a green icon.

Severity in the Web user interface

Each alert type uses a different value to determine the severities of alerts displayed in the Web user interface. For event notifications (email, SNMP, syslog, and SiteProtector), the value is determined by the alert type value in conjunction with the alert configuration for that behavior. When an aggregate is involved, the severity value is the maximum severity associated with its members.

Severity for alert types

The severity values for each alert type are determined as follows:

Alert Type	Value
Client	The severity of the source IP address.
Server	The severity of the destination IP address.
Service	The severity of the port.
Host Pair	The maximum of the source and the destination IP address severity settings.
Connection	The maximum of the source, destination, and port severity settings.
Rate alerts	The severity of the PFCAP expression.

Table 23: *Severity for alert types*

Examples

Violated client alert example

The alert configuration has a severity setting of 6. The client is a member of a group with a severity setting of 3. The server and service have no impact on severity. Notifications for this event will have a severity of 6.

When you look at the Web user interface, the severity you see depends upon how you view the alert:

- If you view as clients, the severity will be 3.

- If you view as something else, all valid fields are counted and the maximum of those will be displayed.

Violated service alert example

The alert configuration for service alerts has a severity setting of 3. The port involved is a member of a port group with a severity setting of 7. Notifications for this event will have a severity of 7. The client in the alert is a member of a group with severity setting of 4, and the server is a member of a group with a severity setting of 5.

When you look at the Web user interface:

- If you view by service, this alert will have a severity of 7.
- If you view as client, the alert will have a severity setting of 4.
- If you view as server, the alert will have a severity setting of 5.
- If you view as hostpair, the alert will have a severity setting of 5.
- If you view as connection, the alert will have a severity setting of 7.

Built-in Behavior Descriptions

Introduction

When you first install Proventia Network ADS, the system monitors your network traffic and gathers traffic data that it uses to build relational, behavioral models of your hosts. When you configure the built-in behavior settings, Proventia sends alert notifications according to the alert configuration settings when it detects violating behavior. This topic describes the different types built-in behaviors.

Worms

A worm is composed of a number of hosts scanning on a single service. Worms scan to propagate on the given service.

Port scans

Port scans are probes to a system to detect open services. These probes may indicate an attacker (or automated malware, such as a worm) searching for vulnerable hosts to attack. Legitimate port scanners may include authorized vulnerability scanners, or other misbehaving applications that blindly attempt connections to many closed ports on a host. For port scans, the system creates one rule and continually builds upon it by adding offending ports to the list.

Host scans

Host scans are network sweeps for hosts running a given service. These sweeps may indicate an attacker (or automated malware, such as a worm) searching for responsive hosts to attack. Legitimate host scanners may include network management systems and authorized vulnerability scanners. For host scans, the system creates one rule and continually builds upon it by adding offending hosts to the list.

Floods

The system automatically creates flood events when it sees traffic floods. It calculates these floods from packet per second violations (based on a two-minute timer) for the following types of rate violations:

Type	Description	Occurs On
TCPSYN	An attempt to open more TCP connections to a destination than it can handle by spoofing the initial packet of a TCP handshake, which fills up the connection table with partially completed connections.	100 pps TCP connections that only have SYN
TCP NULL	A bandwidth exhaustion attack where the attacker sends anomalous TCP segments with no control bits set.	100 pps TCP connections without flags
ICMP	A bandwidth exhaustion attack where the attacker leverages zombie computers to send traffic to many destinations which all respond to the victim.	100 pps for ICMP protocol traffic
IGMP	A bandwidth exhaustion attack using IGMP datagrams to flood the victim.	
IPFRAG	An attempt to exhaust the resources associated with the IP fragment reassembly queues on the target, or trigger known reassembly bugs in certain vendor TCP/IP stacks.	5,000 pps excessive TCP or UDP fragmented traffic

Table 24: *Flood descriptions*

Type	Description	Occurs On
IPNULL	a bandwidth exhaustion attack where the attacker sends anomalous IP datagrams with an invalid IP protocol of zero	100 pps of IP protocol 0

Table 24: *Flood descriptions (Continued)*

ATF rules

The system creates ATF rules automatically from the ISS Active Threat Feed to alert you to Internet threats that could affect your network.

System events

The system event behavior category includes two types of events. The Analyzer sends Collector Up/Down events when it stops receiving data from its Collectors. It creates Miscellaneous System events when it detects Proventia Network ADS health-related system alerts, such as error conditions and warnings when the software certificate is nearing its expiration date.

Built-in behaviors and user-defined rules

Every Proventia Network ADS rule has its own associated alert configuration. Each time you create a rule, the system applies the built-in behavior alerting settings to it, unless you have specified other settings that apply to that particular rule.

Reference: For more information about creating user-defined rules, see "Creating and Editing Rules" on page 117.

Built-in Behavior Alerting

Introduction

This topic provides the instructions for defining global alerting for the built-in behaviors and system events listed on the Policy page.

Prerequisites

Before you configure alerting for the behaviors, you should configure notification objects and time objects so that you can use them in your alerting settings. You might also want to create group objects to use in your alerting settings. This is optional and you can create the alerting settings and then add group objects to them later.

Reference: See "Adding and Editing Notification Objects" on page 41.

Reference: See "Adding and Editing Time Objects" on page 47.

About the global Alert and Notification Configuration page

The system displays fields in the top section of the page that apply globally to all default alerts for the behavior. These settings include enabling alerting for the behavior, selecting the corresponding severity, selecting the time objects during which ADS should consider matching behavior a violation, and selecting the notification objects that ADS should notify when it detects these violations.

Note: Some behaviors do not have alert type settings, such as Collector Up/Down alerts and Miscellaneous System alerts.

Reference: See "Types of alerts" on page 22 for more information.

Viewing the Alerting table

The system displays each alert type in the Alerting table with the current configuration. Each column in the table is field in which you can update your settings, as follows:

Column	Description
Type	The alert type. See "Types of alerts" on page 22 for descriptions.
Groups	Indicates which group objects this alert applies to, and allows you to select additional group objects.
Alerting	Indicates whether alerting for this type is enabled or disabled.
Severity	The selected relative severity the system associates with alerts of this type.
Alerting timeframe	The time objects associated with this alert type. The system only considers the traffic to violate this behavior if it occurs during the configured time object. See "How Proventia Network ADS Determines Severity" on page 60.
Notify Destinations	The notification objects associated with this alert type. The system sends alerts to the members in each notification object. See "How Proventia Network ADS Determines Severity" on page 60.
Selection box	Use this check box to select and delete alerts.

Table 25: *Alerting table*

Configuring Alerting Settings for Built-in Behaviors

Introduction

This topic explains how to configure the alerting settings for built-in behaviors and system events.

User access

Administrators can perform all actions described. Regular users and analysts can view the alerting configuration but cannot edit it.

Adding alert type entries

After you configure the default settings that apply to the overall behavior then you can add alert entries that are appropriate for the behavior, in the Alert Configuration table. The system only displays the alert types that make sense for each behavior. For example, you cannot have Host Pair alerts for a worm.

Configuring global alerting settings for system events

Any global alert settings you configure apply to future Collector Up/Down and Miscellaneous System alerts. They do not apply to alerts ADS has already generated.

To configure default alert settings for system event built-in behaviors:

1. Click the behavior or event name link to navigate to the Edit Global Notification and Alerting or the Configuration for Event page.

   Note: The page names vary depending upon the type of behavior but the pages function the same.

2. Do one of the following:
   - Select **Enabled** from the **New Notification** list to turn alerting on for the behavior.
   - Select **Disabled** if you do not want the system to generate events and alerting notifications for this behavior, and then click **SAVE** to return to the Policy page.
3. Select the severity level you want the system to associate with that type of behavior from the **New Severity** list.

   Note: A setting of 1 is the least severe and a setting of 10 is the most severe.

   Reference: See "About severity settings" on page 60.

4. Select the notification objects that include the network operators that should receive notifications from the **Notify Destinations** list.

   Tip: Press and hold the CTRL key to select multiple notification objects.

Configuring alert types for the behavior

You can add multiple types of alerts for each behavior and assign different settings to each, but you cannot add rate alerting settings for the built-in behaviors.

To configure the settings for each alert type listed or to add an entry:

1. Choose which types of alerting you want to configure by selecting an entry type from the **Add Rate Alerting** list.

   A new row appears in the Alerting table.

2. Do one of the following to select the group objects this alert type applies to:
   - Type the group name in the text box.
   - Click the group selection icon, and then select the option buttons for those groups you want to include, and then click **SAVE**.

3. Select **Enabled** from the **Alerting** list.
4. Select the time object from the **Alerting Timeframe** list that you want the system to use to determine if the behavior is an alert.

   Tip: To select multiple time objects, press and hold the CTRL key, and then select the objects you want to include.
5. Click the Edit link to add or change time objects.

   Reference: See "Adding and Editing Time Objects" on page 47.
6. Select the notification objects you want the system to send alerts to from the **Notification** list.

   Tip: To select multiple notification objects, press and hold the CTRL key, and then select the objects you want to include.

   Important: If you have SiteProtector configured, ADS always sends notifications to SiteProtector. Any notification objects you select from the Notification list are additional.
7. Click the Edit link to add or change notification objects.

   Reference: See "Adding and Editing Notification Objects" on page 41.
8. Click **SAVE** when you finish configuring all alert types for this behavior.

   The Alerting page appears and you can continue to configure settings for additional behaviors.

   Note: You cannot delete rows the system automatically displays for each behavior. If you do not want the system to detect and send notifications for them, disable their Alerting settings.

Configuring Alerting Settings for ATF and User-Defined Rules

Introduction

This topic explains how to configure the alerting settings for ATF and user-defined behaviors.

User access

Regular users and analysts can view the alerting configuration but cannot edit it.

Multiple alert types for behaviors

You can add multiple types of alerts and associate each with different time and notification objects.

Example: You can set New Client alerting for a group and send notifications of violations to one destination for a particular time, and then set another New Client alerting entry but specify a different group.

Adding or editing alerting settings

Any alert settings you configure apply to future alerts. They do not apply to alerts the system has already generated.

To edit or add alerting settings:

1. Go to the Edit Alerting Configuration page.

   Click the name link in the Behavior column to go to the Rule Editor page, and then click **EDIT ALERT CONFIGURATION**.
2. Select the type of alerting you want to configure from the **Add Rate Alerting** list.
3. Do one of the following to select the group objects this alert type applies to:
   - Type the group name in the text box.
   - Click the group selection icon, and then select the option buttons for those groups you want to include, and then click **SAVE**.
4. Select **Enabled** from the **Alerting** list.
5. Select the **Severity** you want the system uses when generating this type of alert.
6. Select the time object from the **Alerting Timeframe** list that you want the system to use to determine if the behavior it sees qualifies as an alert.

   Tip: To select multiple timeframes, press and hold the CTRL key, and then select the timeframes you want to include.
7. Click the Edit link to add or change time objects.

   Reference: See "Adding and Editing Time Objects" on page 47.
8. Select the notification objects you want the system to send alerts to from the **Notification** list.

   Tip: To select multiple notification objects, press and hold the CTRL key, and then select the notification objects you want to include.

   Important: If you have SiteProtector configured, ADS always sends notifications to SiteProtector. Any notification objects you select from the Notification list are additional.
9. Click the Edit link to add or change notification objects.

   Reference: See "Adding and Editing Notification Objects" on page 41.

10. Click **SAVE** when you are finished.

Note: You can not delete rows the system automatically displays for each behavior. If you do not want the system to detect and send notifications for them, disable alerting for the behavior.

Deleting alert entries

When you delete alerting configuration, the system immediately stops generating future events (alerts) for that alert type. Any existing events generated from the alerting settings remain until you delete them from the Event Detail page.

To delete alert entries:

1. Select the check box for the corresponding row(s) you want to delete
2. Click **DELETE**.

Configuring Rate Alerting

Introduction

You can add rate alerts as part of global alerting settings and user-defined rules.

Over rate alerts

The Over setting allows you to choose a rate of traffic that the system uses to generate traffic alerts. It triggers an alert any time it sees traffic that exceeds the allowable rate triggers, during the set timeframe.

Under rate alerts

The Under setting causes the system to generate an alert anytime it sees traffic under the allowable rate during the set timeframe. You can choose from bits per second, flows per second or packets per second ranges for both of these alert types

Monitored rate alerts

You can configure the system to alert you when the traffic exceeds this rate by an amount that you specify, expressed as a percentage. The system sends alerts when the traffic exceeds that amount and during a specified period of time. You can also enter a minimum setting for the system to use in conjunction with this rate. When you specify a minimum rate, the system first looks at the percentage setting. If the traffic exceeds the percentage, but does not exceed the minimum rate, the system does not generate an alert. If the system sees traffic that exceeds both settings and occurs during the set time specification, it triggers an alert and sends it to the members in the selected notification objects.

Setting over and under rate alerting

To set rate alerts:

1. Select **Over Rate Alerts** or **Under Rate Alerts** for the type of rate alert you want to add from the **Add Alerting** list.

   The system displays a new corresponding row in the Alerting table.
2. Type a number in the Over and Under boxes.
3. Select the corresponding rate type from the list (bps, pps, or fps settings).
4. Turn the alerting to **Enabled**, and then select the severity, alerting timeframe, and notification objects that apply to this type of alert.

   Reference: See "Adding or editing alerting settings" on page 67 for these instructions.
5. Repeat Steps 1 through 4 for additional entries.
6. Click **SAVE** when you finish adding all alerting entries for this rule.

Setting profiled rate alerting

To set profiled rate alerts:

1. Select **Profile Rate Alert** from the **Add Alerting** list.

   The system displays a new corresponding row in the Alerting table.
2. Enter a number in the percentage box (%) that represents the percentage of traffic that exceeds the established rate.
3. Enter a whole number in the text box, and then select a corresponding rate setting from the list, to further define when the system sends profile alerts.
4. Turn the alerting to **Enabled**, and then select the severity, alerting timeframe, and notification objects that apply to this type of alert.

   Reference: See "Adding or editing alerting settings" on page 67 for these instructions.

5. Repeat Steps 1 through 4 for additional entries.

Configuring Active Threat Feed Settings

Introduction

The ISS Active Threat Feed (ATF) provides you with information about Internet-wide attacker activity as it relates to your network. When you enable ATF, the system can automatically create behaviors and send notifications for events it detects from ATF updates. The ATF program can create behavior rules for any worm, scan, or other traffic violation or suspected violation it detects. The ATF program also creates events when it detects changes in allocated dark IP space and peer-to-peer changes.

How the ATF data is collected and updated

The ISS security team gathers information for current and emerging threats from a wide range of sources, and incorporates the information into a database of threat profiles maintained on the ATF server. The ATF database is maintained by the ISS security team and can only be accessed by current Proventia Network ADS customers. The ATF server uses your client certificate to authenticate for an SSL session to allow you to download the updated feed.

Note: For ATF server access, your Proventia Network ADS Collector must have a valid DNS server that can contact the ISS DNS server (for valid name resolution).

Preconfigured ATF behaviors

Proventia Network ADS comes preconfigured with some ATF rules that serve as default behaviors for common back doors. These backdoors include several common worms and Trojans (for example, Bagle, Blaster, Dabber, Gholame, Kibuv, and Sasser) and remote administration tools (for example, Back Orifice and Subseven).

Configuring ATF settings

To configure your ATF settings:

1. Select the Enable ATF Updates check box.

   The **Update Interval Period** box appears.

2. Enter a whole number that represents hours from 1-168 (7 days), in the ATF Update Interval box. The Proventia Network ADS uses the interval to determine how often to check the ATF server for updates to the threat feed data

   The default is 1 hour.

3. Do one of the following:
   - Click **SAVE** to save the settings and poll the ATF server at the next set interval.
   - Click **UPDATE NOW** to immediately poll the ATF server and update the information, and then click **SAVE**.

Deleting ATF behaviors

The ATF tables allow you to delete behaviors that you no longer want ADS to detect. The policy remains in the table in case you want to recreate it in the future, but that behavior no longer triggers events or alert notifications.

To delete an ATF behavior:

1. Select the check box on the behavior row(s).
2. Click **DELETE**.

Recreating deleted ATF behaviors

If you delete an ATF behavior, the system stores the information. It continues to display it as an entry in the ATF table, but it no longer displays the behavior name as a link. This

means you cannot edit the settings and the system is no longer actively monitoring for that behavior.

To recreate the behavior and its associated rules:

- Click **RECREATE** on the ATF behavior row.

ATF settings in the CLI

There is one additional setting that you cannot configure in the Web user interface. This setting is configuring a proxy that your Analyzer can pass through to get updated ATF data.

Reference: For these instructions, see the *Proventia Network ADS 3.5 Advanced Configuration Guide.*

Chapter 10

Configuring Worm Protection Settings

Overview

Introduction

Use the Worm Protection Settings page to configure Proventia Network ADS to integrate with your existing CheckPoint firewalls or Cisco Catalyst 6500 (Cat6k) Series switches. When you configure worm settings and enable enforcement, Proventia Network ADS can automatically apply ACL rules to your firewalls that filter out unapproved traffic, while still allowing the legitimate traffic on your network.

Worm Settings page views

When you choose Worm Protection Settings from the Settings menu, the page that Proventia Network ADS displays depends upon the device type you select:

- Cat6k
- CheckPoint

Note: You can only configure one Enforcement Device Type for each Analyzer.

User access on the Worm Protection Settings page

Administrators can perform all actions described in this chapter. Users and analysts can view worm protection settings, but cannot change them.

In this chapter

This chapter contains the following topics:

Configuring Cisco Catalyst 6500 Series Switch Settings

Introduction

You must configure worm settings to enable automatic worm rule enforcement. This section provides the instructions for configuring your Cisco switches and routers to enforce worm rules.

Cisco supported hardware

Proventia Network ADS supports integration with the following Cisco hardware:

- Cisco 7600 Series routers
- Cisco Catalyst 6500 Series switches that are equipped with both:
  - A Policy Feature Card (PFC, PFC2, or PFC3)
  - A Multi-Layer Switching Feature Card (MSFC, MSFC2, or MSFC3)

About the CAT6K Worm Settings page

The Cat6K Worm Settings page displays the settings that apply to all switch configuration in the upper pane. The lower panes show configured switches and allow you to add new switches and routers.

Configuring Cisco switch settings

These settings are overall settings that Proventia Network ADS applies to all switches you add.

To configure the Cat6K settings on the Analyzer:

1. Select one of the following option buttons for the type of rules you want the system to generate:
   - Client-server rules
   - Server
2. Select the **Cat6K** enforcement device option.
3. Type the number of filters you do not want the system to exceed for each device in the **Max Filters per Device** box.
4. Type the Cat6k reserved ACL numbers in the **1st** and **2nd** boxes.

   Proventia ADS uses those numbers when it starts assigning ACL rules.
5. Click **SAVE**.

Adding a Cisco Catalyst 6500 series switch

To add a switch:

1. Type a name that helps you identify the switch in the **Cat6k Name** box.
2. Type the switch (or router) **IP Address**.
3. Select one of the following login method that you want your Analyzer to use to connect to the switch.
   - Telnet
   - SSH
4. For SSH access, you can type a key in the **Host Key** box.

   This setting is optional.

   Note: If you enter a host key, then Proventia Network ADS generates an alert any time it detects a host key change.

5. Type your **Login Username**.

   This is required for SSH login.

6. Type your **Login Password** to view the switch.

   This is required for SSH login.

   After you set this, the system displays "is set" in the Cisco CAT6K Switches table.

7. Enter a password that enables you to access the switch in privileged mode in the **Enable Password box**.

   After you set this, the system displays "is set" in the table in the upper pane.

8. Type the name of the switch/router interface in the **In** box. This setting specifies the interface on which ADS filters the traffic as it travels into the interface.

   Example: VLAN112

   Tip: Type multiple In interfaces as a comma-separated list.

   Important: You can configure both an In and Out interface, but you must configure at least one.

9. Repeat the instructions in Step 8 to configure the **Out** interface.

10. Click **ADD**.

    Proventia Network ADS displays the switch in the Cisco CAT6k Switches table and displays a new row for you to enter another switch.

Editing Cisco switch settings

To edit switch settings:

1. Click the switch name link in the Cisco Cat6K Switches table.

   The switch settings appear in the Edit pane for you to change.

2. Type the new information in the appropriate boxes.

3. Click **UPDATE** to save the new configuration.

   The updated information appears in the Cisco Cat6k Switches table.

Deleting Cisco switches

To delete a switch:

- Select the check box on the switch row, and then click **DELETE**.

Configuring CheckPoint Settings

Introduction

This section provides the instructions for configuring your CheckPoint Open Platform for Security (OPSEC) firewalls to enforce worm rules.

Pre-requisites

Before you configure your Proventia Network ADS Analyzer and your Check Point system to integrate for Safe Quarantine, you must configure your Check Point SMART management console to allow Proventia Network ADS secure access to your firewalls.

Reference: See "Check Point Integration for Safe Quarantine" in the *Proventia Network ADS Advanced Configuration Guide*.

Getting information from your CheckPoint SMART management console

Your Proventia Network ADS Analyzer must have the following information from the CheckPoint SMART management console so that it can retrieve the certificate, enabling the two to communicate:

- the console server's IP address
- the Check Point Secure Internal Communications (SIC) distinguished name (DN)
- the Proventia Network ADS Secure Internal Communications (SIC) distinguished name (DN)

By default, Proventia Network ADS communicates with the Check Point SMART management console using secure sockets layer certificate authority (sslca) authentication on TCP port 18190.

Procedure

To configure your CheckPoint settings on the Analyzer:

1. Select one of the following option buttons for the type of rules you want the system to generate:
   - Client-server rules
   - Server
2. Select the **CheckPoint** enforcement device option.
3. Type the number of filters you do not want the system to exceed for each device in the **Max Filters per Device** box.
4. Click **SAVE**.

Next, configure the settings to allow communication. You only need to configure these settings once, unless you want to change them in the future.

Configuring communication

To configure the settings to allow communication:

1. Type (or copy and paste) the **Check Point SMART Management console IP** address from your Check Point configuration.
2. Type (or copy and paste) the *Check Point management console SIC DN* from your Check Point configuration.
3. Type (or copy and paste) the **System SIC DN** for your Analyzer from your Check Point configuration.

4. Type the **Activation Key**.

   Tip: This must be the same key you entered on the Check Point SMART management console.

   Proventia Network ADS uses this one time to retrieve the certificate; it does not store or display the key.

5. Click **GET CERT**.

   Proventia Network ADS retrieves the certificate from your Check Point SMART management console and displays the information (except for the activation key) statically. It no longer displays the entry fields.

Changing the settings

You must clear the current certificate if you want to change either the certificate or other settings.

Important: If you clear the certificate, you cannot retrieve it again from the same management console until you have reset the secure internal communication (SIC) trust state.

To clear the saved information:

- Click **CLEAR CERT**.
- Proventia Network ADS clears the certificate and your current settings, and then displays entry boxes so you can enter the new information.

Chapter 11

Configuring Port Objects

Overview

Introduction

Use the Port Object Configuration page to group like ports (for example, all ports used for connecting to the Web) together. This is useful for searching and alerting purposes. You can set the severity levels for critical ports or services, so the system ranks and displays associated alerts with a higher severity level.

User access

Administrators can perform all actions described in this chapter. Analysts can create and edit port objects. Users can view the port configuration, but they cannot edit it or add change messages.

In this chapter

This chapter contains the following topics:

About the Port Objects Configuration Page

Introduction

The Port Objects Configuration page displays all of the configured objects and their settings.

Navigating and searching on the Port Objects page

Standard navigation and searching apply on the Port Object Configuration page. You can search by object name, creator, or member names, and import and export port object files.

Reference: See "Navigating the Proventia Network ADS Web User Interface" on page 12.

Port objects table

The Port table shows the following information for each group listed on this page:

Column	Description
Port Object Name	The name of the port object, as a link to its Edit page.
Severity	The user-assigned severity level Proventia ADS uses when creating alerts that involve this group.
Members	The names or addresses of the group members. If the number of members exceeds five lines, this column shows an ellipsis point link (...) that you can click to navigate to the Edit page to see the complete list of members.
Comment	Any comments entered when the group object was created.
Log Message	The most recent logged message for this group object.
Creator	The name of the user who created the group object.
Last Modified	The last time the group was changed (this includes system-generated changes).
Rule Referrers	The names of all rules that reference this group object, as links to the Edit page
Selection check box	Use to select specific rows to delete.

Table 26: *Port objects table*

About change messages

You should enter a change message when you make changes to a port object. The system displays these messages as part of the log pages and the recent changes for reference.

Viewing recent changes

The Port Objects Configuration page displays a list of the most recent notification changes for you to reference. To see a complete list of all notification object changes:

- Click the Full change log for Port Group Object link to navigate to the Log Detail.

Adding and Editing Port Objects

Introduction

This topic provides the instructions for adding and editing group objects. Because the pages for adding and editing port objects are similar, they are addressed here together.

Naming port objects

When you add a port group, you assign it a name. ISS recommends assigning each object a unique name that allows you to easily identify its members. You can use the same characters that are allowed for creating group objects.

Reference: See "Naming group objects" on page 51 for a list of valid characters.

Procedure

To add or edit port objects:

1. Do one of the following to navigate to the Edit page:
   - Click **NEW PORT OBJECT** to add a new object.
   - Click the name link to change the settings for an existing port object.
2. Type a name for the group object in the **Name** box.

   Reference: See "Naming group objects" on page 51 for a list of all valid characters.
3. Type any comments that describe the port object or that help you identify it in the **Comment** box.

   Proventia Network ADS displays the text you enter here in the Comment column on the pages that include port objects in the data tables.
4. Type the members as a port number or service name for the ports you want Proventia Network ADS to monitor in the **Members** box.

   Tip: Enter multiple ports as numbers either separated by a comma, or on a new line.

   The system matches both UDP and TCP with the port numbers you enter.

   Example: If you enter port 80 as a member of a port object, the system groups traffic on TCP port 80 and UDP port 80.
5. Select the severity you want to associate with this object.

   Note: When this object is involved in alert traffic, the system uses this setting to flag the alert (unless there is a higher setting associated with the alert). The system always uses the highest setting when sending alerts.
6. Type any messages that describe your changes in the **Change Message** box.

   These messages appear in the log pages that include this port object.
7. Click **SAVE**.

Importing and Exporting Port Object Files

Introduction

When you add or edit a port object, you can import existing comma-separated value (CSV) files that you can use to create new groups or merge into existing groups. Exporting a port object file allows you to see an example of the file format or to the backup your network configuration within the system. You can also import and export a port file to use when setting up a new Proventia Network ADS system or for archival purposes.

CSV port object file format

Each port group in the CSV file has the following seven attributes, in order, separated by commas, and within quotation marks (for comments and log messages):

- port object name
- severity
- creator
- last modified
- comments
- log message
- list of port numbers

Examples:

console,3,,,"telnet and ssh ports","creating port group...","21,22"

user,3,,,,,"1025-65535"

How Proventia Network ADS merges imported ports

This table shows how Proventia Network ADS merges imported ports:

If the port...	Then ADS...
exists, but is different	updates (overwrites) the old information
exists, but is the same	ignores the new information.
does not exist	adds the new information.

Table 27: *Merge results for port objects*

Importing port object files

To import a file:

1. Do one of the following:
   - Enter the file name in the box.
   - Click **Browse**, and then select the file to be included.
2. Type a description that explains why or what objects you are importing in the **Change Message** box.
3. Click **IMPORT**.

   The system displays a confirmation message when it finishes importing, and then shows the new port information in the port objects data table.

Exporting port object files

To export a file:

1. Type a description that explains why or what objects you are exporting in the **Change Message** box.
2. Click **EXPORT**, and then specify how you want to save or open the file, according to the choices your browser displays.

   Proventia Network ADS generates an XML report containing the port list to the location you specify.

Deleting Port Objects

Introduction

Delete groups on the Configure Port Objects page.

Deleting ports with rule referrers

If you delete a port object that is part of any policy rules, the system displays a message showing you the number of rules this port object refers to.

Procedure

To delete a port object:

1. Select the check box on the object row in the table.
2. Type a description that explains why you are deleting the object in the **Change Message** box.
3. Click **DELETE**.

   If the system displays the rule referrer message, click **OK** to delete the port object.

Chapter 12

Configuring General Settings

Overview

Introduction

Use the General Settings page to set your global system preferences, and to export the current configuration to a file, or upload and restore the most recently saved configuration.

User access for general settings

Administrators can perform all actions described in this chapter. Analysts cannot edit DNS, NTP, or SMTP server configuration, but they can backup and download the system configuration. Users can view the system configuration but can not make changes or backup and restore configuration.

In this chapter

This chapter contains the following topics:

Configuring General Settings

Introduction

This topic describes each general setting and tells how to set them. General settings include setting your DNS servers, your NTP servers, your SMTP server, and the SNMP agent.

About DNS servers

DNS servers specify the servers that provide domain name service mappings from IP addresses to host names in Proventia Network ADS. You can set multiple DNS servers. The system tries the first IP address listed as the primary name server, and then it tries the subsequent ones listed as backup name servers.

About the SNMP agent community

Proventia Network ADS allows external sources to SNMP query Proventia Network ADS for the following system status and configuration information:

- Disk Space Free/Used (for Analyzer/Collector)
- Current Flow Log Size
- FPS for each Collector
- Proventia Network ADS configuration (includes accounts, group objects, port objects, rules and enforcement device information)

By default, external sources can poll your Analyzer. If you do not want to allow this, configure a unique SNMP Agent Community that external sources will not guess.

Procedure

To configure general settings:

1. Type the IP addresses of your DNS servers in the **DNS Servers** box.

   Tip: Enter multiple DNS servers as a comma-separated list of IP addresses.
2. Enter the NTP server's IP address in the **NTP** box.
3. Type the IP address for the SMTP relay you want the system to use to send email notifications, in the **SMTP** box.
4. Type the community string in the **SNMP Agent Community** box if you do not want to allow external sources to poll your Analyzer. Otherwise, you can leave this box empty.
5. Click **SAVE**.